UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA,

Plaintiff,

-v-

ROSS WILLIAM ULBRICHT,

Defendant.

----------X

14 Cr. 68 (KBF)

DECLARATION OF
ANDREW J SAYLER

I, Andrew Sayler, pursuant to 28 U.S.C. § 1746, hereby affirm under penalty of perjury:

1. I am a computer scientist specializing in information security, computer systems, and technology policy. I have worked or studied in the field of computer security for over eight years. I hold both a PhD and MS in Computer Science and a Bachelors of Science in Electrical Engineering with a minor in Computer Science. My resume is attached. Exhibit 1.

2. I am familiar with network security analysis, including the analysis of network traffic captures such as pcap files. I am also familiar with Internet architecture and the operation of computer networks.

3. I examined pen register and trap and trace data provided to me as pcap files by Paul Grant, attorney, who advised me that he represents Ross Ulbricht in this case.

4. The pcap files appears to contain wide-area network (WAN) traffic involving communications between a cable modem and other servers on the Internet. These files show bidirectional traffic, but always involve a Comcast IP address (67.169.90.28) as one end of each exchange. Since the

traffic all appears to be between a modem and other systems on the Internet, it could have been collected by Comcast outside the home without needing to break any WiFi encryption or otherwise monitor the home's local-area network.

5. None of the pcap files provided to me appear to contain local-area network (LAN) or WiFi traffic internal to the house where the modem was located.

6. None of the pcap files provided appear to identify any of the MAC addresses internal to the home network or WiFi. They only show the external MAC address of the modem itself, plus the MAC addresses of other Internet systems, most likely routers on Comcast's network. All of the internal MAC addresses (for devices on the home network) would have been stripped from this traffic by the home's router or modem before the traffic entered Comcast's network where it appears these data were collected.

7. There is no way to know who within the house originated the network traffic I examined from the traffic alone. It appears to be an amalgamation of all the Internet traffic sent or received by every active device connected to the home's network at the time of collection. There is no way to know if this traffic is limited to a single individual or is from multiple individuals absent additional information about who and what devices were present on the network at the time of its collection.

8. I have read through two court orders authorizing pen register and trap and trace data collection from Comcast: 13 MAG 2228 (9/16/13) and 13 MAG 2236 (9/17/13). The pcap files I examined appear to correspond to the 13 MAG 2236 (9/17/13) order which references the 67.169.90.28 IP address seen in the files. The earlier order references a second IP address (67.170.232.207) that does not appear to be the focus of the pcap files I was provided.

9. I have also examined additional pen register and trap and trace data that Paul Grant provided to me in a csv (comma-separated value) format. Those csv files appear to contain a processed version of the same pcap data previously examined. As such, they do not present any significant new information beyond that provided by the pcap files and lead to the same conclusions.

10. I reviewed the affidavit of Christopher W. Tarbell (the "affiant"), an affidavit provided as part of the application for the laptop search warrant. In his affidavit, the affiant describes the "SUBJECT COMPUTER" as a silver Samsung laptop computer, containing a network adapter assigned the MAC address of 88-53-2E-9C-81-96, and states that computer was known to be used by Ross William Ulbricht. Affidavit at ¶5.

11. In his affidavit, the affiant further describes how the FBI used pen register and trap and trace data they collected from the LAN-side of the home's wireless router to identify the MAC address associated with Ulbricht's laptop (¶35).

12. I have reviewed the "Wireless Routing Pen" application the government requested on September 20, 2013, and that Order mentions that the FBI was seeking a pen-trap order to collect any MAC addresses associated with communications sent to or from the wireless router maintained at a certain address. See 13 MAG 2274. I also reviewed a second pen-trap order (13 MAG 2275) on that same date that allowed the government to capture communications from any computers associated with any of four different MAC addresses.

13. None of the data I examined show any of the described LAN-side data collection, nor did it show the identification of any MAC addresses of any devices on the LAN network. I have seen no data which shows that any MAC addresses were collected by the government's efforts pursuant to either pen-trap order, let alone the MAC address which the affiant claims is

associated with the SUBJECT COMPUTER. I have seen no data which show any communications to or from any devices associated with any of the MAC addresses mentioned in the orders or the affidavit. It is not clear from the data I have been provided how the FBI obtained the MAC address of Ulbricht's laptop.

14. In his affidavit, the affiant described a "MAC address" as "a unique identifier assigned to the network interface on a computer device, which provides a means of identifying the device on a network." Affidavit, fn1.

15. Based on my education and experience, I disagree with the affiant's statement regarding the uniqueness of a MAC address and, therefore, with the value of a MAC addresses for the purpose of identifying a device on a network. I know from my own study and work that changing a MAC address is a trivial operation on most systems. I have published an article on that subject. See Andy Sayler, *Network Anonymity Through "MAC Swapping"*. (An article appearing in 2600: The Hacker Quarterly, Volume 28, Issue 3, Autumn 2011. Middle Island, NY.)

16. I understand that when Ulbricht's laptop was seized, it was running Ubuntu Linux. Tr 856 - 858. On Ubuntu Linux it would have been a trivial step to change the MAC address of the laptop. Ulbricht could have collected other MAC addresses on any network he used, and then substituted other MAC addresses for his own. Similarly, other users on networks used by Ulbricht could have collected the MAC address from Ulbricht's computer, and used his MAC address as their own. Due to these capabilities, a MAC address is not a robust, unique identifier of a device on a network. The fact that MAC addresses can be easily changed is widely known.

17. The affiant also stated in fn2, that "every computer device on the Internet has an Internet protocol or 'IP' address assigned to it, which is used to route Internet traffic to or from the

device. A device's IP address can be used to determine its physical location and, thereby, its user."

18. Based on my education and experience, I disagree with this statement. First, most devices connect to the Internet via a router or gateway that performs network address translation (NAT). This process allows multiple local network devices (laptops, phones, etc.) to all share a single public IP address. Thus, a public IP address is often not unique to a single device, but is instead shared by multiple devices within a single home network. Furthermore, public IP addresses assigned by an ISP such as Comcast are not permanent. They tend to change with regular frequency, meaning an IP that corresponds to a collection of devices on one home network today may be used by a separate home and its devices tomorrow. These facts are widely known and not new. Finally, there are numerous ways to change a device's public IP address such as anonymity networks like Tor or virtual-private networks (VPNs). These methods are commonly used to enhance user privacy or to change the apparent location of a device. The affiant himself provides an explanation as to how the Tor network conceals the true IP addresses of computers on the Internet. Affidavit at ¶5 b i. The affiant also states he knew that IP addresses can be assigned by a VPN. Affidavit at ¶28 c. Such assignments are temporary and easily changed. The affiant's own assertions contradict his statement in fn2 that an IP address is a reliable identifier of a user or their location.

19. In his affidavit, the affiant states that the first six characters in the SUBJECT COMPUTER MAC address indicate that the SUBJECT COMPUTER is a Windows-based computer. ¶36. I have seen no data that would support that conclusion. Furthermore I disagree that the MAC address of a device reliably indicates what operating system is running on the device. The MAC

address noted in the affidavit (88-53-2E-9C-81-96) appears to correspond to an Intel network device. Intel devices are routinely used by systems running Windows, Linux, or other operating systems, and are not unique to Windows. These facts are also commonly known in the industry.

20. In his affidavit, the affiant states that DPR had provided directions to Silk Road administrators for how to install Pidgin (a chat program) from an ".exe" file (a format common to Windows machines), and that these are likely the directions DPR himself followed to install Pidgin, providing further evidence that DPR used a Windows machine. Affidavit at ¶37. I find this conclusion to be unsupported. The mere fact that DPR was explaining how to install a program on Windows to other users in no way indicates that he himself used Windows. Indeed, I regularly provide directions for installing programs on Windows to other users despite the fact that I most frequently use Linux. The Pidgin chat program also runs on multiple operating systems, including macOS (Apple), Windows, and Linux, making it impossible to determine what operating system a person is running merely from knowledge of Pidgin's use.

21. The affiant stated that the SUBJECT COMPUTER was the only Windows-based computer detected from the Wireless Routing Pen. Affidavit at ¶36. As noted above, I see no basis for the affiant to claim that he knew that the SUBJECT COMPUTER was a Windows-based computer. The assertions the affiant offers to support his conclusion that the device was a Windows computer are flawed and inaccurate. Indeed, the fact that Ulbricht's laptop was actually found to be running Ubuntu, and not Windows, is not surprising given these flaws in the affiant's statement.

22. The affiant stated in his affidavit that the FBI collected data on September 20, 2013, that showed the SUBJECT COMPUTER connecting to the wireless router at the subject residence.

Affidavit at ¶39. I have not seen any such data, and I have seen no basis for the affiant to claim that the FBI had collected data that showed anything communicated to or from the SUBJECT COMPUTER.

23. I have disagreements with many of the affiant's statements of fact that were provided in the search warrant affidavit, including those mentioned above. I have seen no data resulting from pen register or trap and trace data collection that supports the affiant's claim to have uniquely identified Ulbricht's computer or any other computer present on the home's network.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 16th day of May, 2019.

Andrew Sayler, PhD

EXHIBIT 1 TO SAYLER DECLARATION

Andy Sayler

www.andysayler.com
andy.sayler@gmail.com

Education

University of Colorado, Boulder, CO — **GPA:** 3.99
PhD in Computer Science - Computer Systems Research Group — ***Spring 2016***
Areas of Research: Security and Privacy, Operating Systems, Networking

Tufts University, Medford, MA — **GPA:** 3.59
BS in Electrical Engineering, Minor in Computer Science — ***May 2011***
Honors: Magna Cum Laude – Engineering Dean's List

Employment

Twitter, Inc - Boulder, CO — ***September 2016 – Present***
Senior Security Engineer - Enterprise Security Team
- Tech lead for the Infrastructure Security Automation and Tooling Group
- Provided security consulting guidance and developed range of security measurement tools

University of Colorado - Boulder, CO — ***August 2011 – August 2016***
Teaching and Graduate Assistant - Dept. of Computer Science
- Designed and administered a variety of educational technology systems for 1000+ CS students
- Taught Computer Systems, Operating Systems, and Development Methods and Tools courses

Center for Democracy and Technology - Washington, DC — ***May 2015 – July 2015***
Policy Technologist - Hatfield Summer Scholar
- Represented security researchers in triannual 17 U.S.C. §1201 (DMCA) proceeding
- Led CDT efforts to reform Wassenaar export control rules related to encryption and security tools

SolidFire, Inc - Boulder CO — ***May 2013 - May 2014***
Development Team Intern
- Created virtualization-based test and prototyping environment for SSD-backed SAN product

Symplified, Inc - Boulder CO — ***June 2012 - August 2012***
Development Team Intern
- Implemented reverse-proxy-based Kerberos and NTLM authentication systems

WMFO 91.5 FM – Tufts Freeform Radio - Medford, MA — ***December 2008 – May 2011***
General Manager
- Oversaw 15 member Executive Board managing a 200 staff-member community radio station

Charles Stark Draper Laboratory - Cambridge, MA — ***June 2010 – August 2010***
Navigation Engineering Intern - Draper Lab Scholar Program Member
- Designed and implemented multi-node distributed ranging navigation simulation

MIT Lincoln Laboratory - Lexington, MA — ***June 2009 – August 2009***
Radar Engineering Intern
- Designed, implemented, and tested network-centric radar (ROSA) software test suite

Special Application Robotics - Loveland, CO — ***May 2008 – August 2008***
Controls Engineering Intern
- Designed, built, and programmed PIC embedded system brushless DC motor control boards

Skills

Computer: Linux, Networking, Security, Firewalls, Virtualization, Systems Administration
Programming: Python, C, C++, Assembly, BASH, LLVM, MATLAB
Other: DevOps, Leadership, Public Policy, Agile Development, Free Software

Awards

TPRC 44 Student Paper Award - First Place	***2016***
Hatfield Summer Scholarship for Public Policy and Service	***2015***
CU "Best Should Teach" Silver Award for Service as CU CS Lead TA	***2014***
CU CS Outstanding Teaching Assistant for TAing Operating Systems Course	***2013***
Tufts Alumni Association Senior Award for Academics and Leadership	***2011***
IEEE TePRA Student Robotics Competition - Second Place	***2009***
Tufts IEEE EE14 Microcontroller Design Project - First Place	***2008***
College Board National AP Scholar	***2007***

Involvement

ACM Member	***2013 - Present***
USENIX Member	***2013 - Present***
EFF Supporter	***2012 - Present***
IEEE Member	***2008 - Present***
CU IT Student Advisory Board Co-chair	***2014 - 2016***
CU Hacking Club Coordinator and Hacking Team Coach	***2012 - 2016***
Tufts Formula Hybrid Racing Team – Lead Electrical Engineer	***2009 - 2010***

Selected Publications

Andy Sayler, et. al. *Tutamen: A Next-Generation Secret Storage Platform*. Symposium on Cloud Computing, 2016. Santa Clara, CA.

Andy Sayler. *Categorizing, Analyzing, and Managing Third Party Trust*. TPRC 44, 2016. Arlington, VA.

Andy Sayler. *Securing Secrets and Managing Trust in Modern Computing Applications*. PhD Dissertation. University of Colorado, Dept. of Computer Science. 2016. Boulder, CO.

Andy Sayler, Dirk Grunwald. *Custos: Increasing Security with Secret Storage as a Service*. Proceedings of the 2nd Conference on Timely Results in Operating Systems, 2014. Broomfield, CO.

Andy Sayler, Dirk Grunwald, et. al. *Supporting CS Education via Virtualization and Packages: Tools for Successfully Accommodating "Bring Your Own Device" at Scale*. SIGCSE, 2014. Atlanta, GA.

Andy Sayler, Eric Keller, and Dirk Grunwald. *Jobber: Automating Inter-Tenant Trust in The Cloud*. Presented at the 5th USENIX Workshop on Hot Topics in Cloud Computing, 2013. San Jose, CA.

Andy Sayler. *Network Anonymity Through "MAC Swapping"*. An article in 2600: The Hacker Quarterly, Volume 28, Issue 3, Autumn 2011. Middle Island, NY.

Additional Information

Personal Website:	https://www.andysayler.com
Github Projects:	https://github.com/asayler
LinkedIn Profile:	https://www.linkedin.com/pub/andrew-sayler/20/8/79a
Google Scholar:	https://scholar.google.com/citations?user=n7fSFIIAAAAJ&hl